Fake-Acknowledgment Attack on ACK-based Sensor Power Schedule for Remote State Estimation

Yuzhe Li[⋆], Daniel E. Quevedo[†], *Senior Member, IEEE,* Subhrakanti Dey[◇], *Senior Member, IEEE,* and Ling Shi[⋆], *Member, IEEE*

Abstract—We consider a class of malicious attacks against remote state estimation. A sensor with limited resources adopts an acknowledgement (ACK)-based online power schedule to improve the remote state estimation performance. A malicious attacker can modify the ACKs from the remote estimator and convey fake information to the sensor. When the capability of the attacker is limited, we propose an attack strategy for the attacker and analyze the corresponding effect on the estimation performance. The possible responses of the sensor are studied and a condition for the sensor to discard ACKs and switch from online schedule to offline schedule is provided.

Index Terms—Cyber-physical Systems, Security, Fake-ACK Attack, Remote State Estimation.

I. INTRODUCTION

Cyber-physical systems (CPS) have been a hot topic among both academic and industrial communities in the past few years. A wide application spectrum of CPS can be found in areas such as smart grid, intelligent transportation and environment monitoring [1] with the integration of sensing, control, communication and computation. In most CPS infrastructures, wireless sensors are key components with advantages such as low cost, easy installation, self-power [2], when compared with traditional wired sensors. Therefore, wireless sensors have been increasingly equipped in CPS to replace wired sensors. The new issues due to their special characteristics have attracted much attention in recent years.

The first issue is how to allocate the energy of the sensor efficiently. Since most wireless sensors use on-board batteries which are difficult to replace, and are typically expected to work for several years without battery replacement, energy conservation is critical [3]–[5]. In [6], the authors consider the sensor scheduling problem of whether it should send its data to a remote estimator or not due to the limited available communication energy. The optimal offline sensor schedule is derived, where the term "offline" means that the sensor designs its strategy before the process starting, i.e., independent of the state of the process. In [7]–[9], the authors extend the result in [6] and propose a so-called "online" sensor power schedules by utilizing the real-time information of the process. One typical category of online information is the ACK from the remote estimator, indicating whether the data packet

⋆: Electronic and Computer Engineering, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong. Email: {yliah, eesling}@ust.hk.
†: Department of Electrical Engineering (EIM-E), The University of Paderborn, Germany, Email: dquevedo@ieee.org.
◇: Department of Engineering Sciences, Uppsala University, Sweden, Email: subhrakanti.dey@angstrom.uu.se.

from the sensor arrives successfully or not. The ACK-based online power schedule is proved to improve the estimation performance significantly [8] compared to the offline schedule which only requires sending a 1-bit ACK packet.
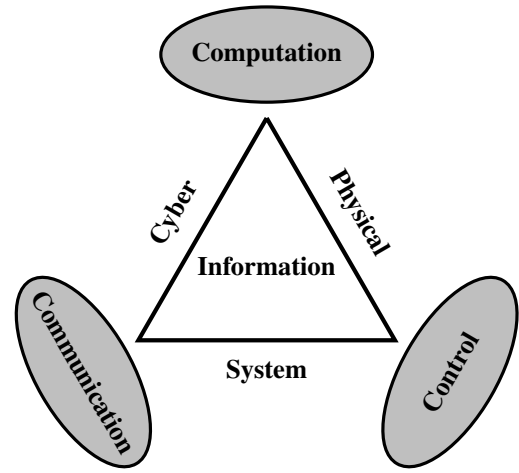

Fig. 1. Architecture of Cyber-Physical Systems.

However, as the communication is through a wireless channel, these sensors are more vulnerable to cyber security threats. In some safety-critical infrastructures, the wide use of CPS enlarges the risks and severities of such attacks. For example, as the largest and most complex CPS in the future, any severe attack on smart grid may have significant impacts on national economy and security or even loss of human life [10]. Therefore, the security issue is of fundamental importance to ensure the safe operation of CPS. There are two possible types of attacks that are commonly investigated in the literature: deception (integrity) attacks and denial-of-service (DoS) attacks [11], corresponding to the two traditional security goals *integrity* and *availability*. The integrity attacks on CPS focus on the integrity of data by modifying the data packet [12], [13], while the DoS attacks block the exchange of information including sensor measurements or control inputs between each part of CPS [14], [15]. In practice, the integrity attacks studied in [12], [13], [16] often require comprehensive information about the system and modifications of the data. Such information is not needed in DoS attacks. In this work, we will consider both types of attacks.

Though the online power schedule in [8] improves the estimation performance, the simple structure of the ACK

packet makes it a more reachable (and likely) alternative for the adversary, under both integrity attacks and DoS attacks. Elucidating what is the possible attack patterns are and how they will affect the estimation performance are important to help us improve the design of CPS. This motivates us to investigate such potential class of malicious attacks against ACK-based remote state estimation.

The remainder of the work is organized as follows. Section II presents the system framework and states the main problem of interest. Section III provides some preliminaries about the optimal offline schedule and an online schedule. The analysis of our proposed fake-ACK attack pattern is given in Section IV. Numerical examples and simulations are demonstrated in Section V. Section VI provides some concluding remarks.

Notations: $\mathbb{Z}$ denotes the set of all integers and $\mathbb{N}$ the positive integers. $\mathbb{R}$ is the set of real numbers. $\mathbb{R}^n$ is the n-dimensional Euclidean space. $\mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$) is the set of n by n positive semi-definite matrices (and positive definite matrices). When $X \in \mathbb{S}_+^n$ (and $\mathbb{S}_{++}^n$), we write $X \geqslant 0$ (and $X > 0$) and $X \geqslant Y$ if $X - Y \in \mathbb{S}_+^n$. The curled inequality symbols $\succeq$ and $\preceq$ (and their strict forms $\succ$ and $\prec$) are used to denote generalized componentwise inequalities between vectors: for vectors $\mathbf{a} = [a_1, a_2, ..., a_n]', \mathbf{b} = [b_1, b_2, ..., b_n]'$, we write $\mathbf{a} \succeq \mathbf{b}$ if $a_i \geqslant b_i$, for $i = 1, 2, ..., n$. $\mathbf{1}$ denotes vector with all entries one. $\mathrm{Tr}(\cdot)$ is the trace of a matrix. The superscript $'$ stands for transposition. For functions g, h with appropriate domains, $g \circ h(x)$ stands for the function composition $g\big(h(x)\big)$, and $h^n(x) \triangleq h\big(h^{n-1}(x)\big)$, where $n \in \mathbb{N}$ and with $h^0(x) \triangleq x$. δ_{ij} is the Dirac delta function, i.e., δ_{ij} equals to 1 when $i = j$, and 0 otherwise. The notation $\mathbb{P}[\cdot]$ refers to probability and $\mathbb{E}[\cdot]$ to expectation.

II. PROBLEM SETUP

A. System Model

Our interest lies in the security of a remote state estimation as depicted in Fig. 2. Here we consider a general discrete-time linear time-invariant (LTI) process of the form:

$$
\begin{aligned}
x_{k+1} &= Ax_k + w_k, & (1) \\
y_k &= Cx_k + v_k, & (2)
\end{aligned}
$$

where $k \in \mathbb{N}$, $x_k \in \mathbb{R}^{n_x}$ is the process state vector at time k, $y_k \in \mathbb{R}^{n_y}$ is the measurement taken by the sensor, $w_k \in \mathbb{R}^{n_x}$ and $v_k \in \mathbb{R}^{n_y}$ are zero-mean i.i.d. Gaussian noises with $\mathbb{E}[w_k w_j'] = \delta_{kj}Q$ ($Q \geqslant 0$), $\mathbb{E}[v_k v_j'] = \delta_{kj}R$ ($R > 0$), $\mathbb{E}[w_k v_j'] = 0 \ \forall j, k \in \mathbb{N}$. The initial state x_0 is a zero-mean Gaussian random vector uncorrelated with w_k and v_k with covariance $\Pi_0 \geqslant 0$. The pair (A, C) is assumed to be observable and $(A, Q^{1/2})$ is controllable.

We consider the so-called "smart sensor" as described in [17], which first locally estimates the state x_k based on all the measurements it has collected up to time k and then transmits its local estimate to the remote estimator.

Denote $\hat{x}_k^s$ and P_k^s as the sensor's local minimum mean-squared error (MMSE) estimate of the state x_k and the
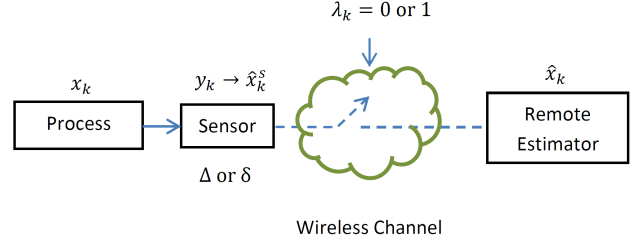

Fig. 2. System Architecture.

corresponding error covariance:

$$
\begin{aligned}
\hat{x}_k^s &= \mathbb{E}[x_k | y_1, y_2, ..., y_k], & (3) \\
\hat{P}_k^s &= \mathbb{E}[(x_k - \hat{x}_k^s)(x_k - \hat{x}_k^s)' | y_1, y_2, ..., y_k], & (4)
\end{aligned}
$$

which can be calculated by a standard Kalman filter.

As the estimation error covariance of the Kalman filter converges to a unique value from any initial condition ([18]), without loss of generality, we assume that the Kalman filter at the sensor side has entered the steady state and simplify our subsequent discussion by setting:

$$
P_k^s = \overline{P}, \ k \geqslant 1, \tag{5}
$$

where $\overline{P}$ is the steady-state error covariance. For notational ease, we define the Lyapunov and Riccati operators $h, \tilde{g} : \mathbb{S}_+^n \to \mathbb{S}_+^n$ as:

$$
\begin{aligned}
h(X) &\triangleq AXA' + Q, \\
\tilde{g}(X) &\triangleq X - XC'[CXC' + R]^{-1}CX.
\end{aligned}
$$

Then $\overline{P}$ is given by the unique positive semi-definite solution of $\tilde{g} \circ h(X) = X$ (see [18]).

The error covariance $\overline{P}$ has the following property:

Lemma 2.1: (Lemma 2.3 in [19]) For $0 \leqslant t_1 \leqslant t_2$, the following inequality holds:

$$
h^{t_1}(\overline{P}) \leqslant h^{t_2}(\overline{P}). \tag{6}
$$

In addition, if $t_1 < t_2$, then

$$
\mathrm{Tr}\left(h^{t_1}(\overline{P})\right) < \mathrm{Tr}\left(h^{t_2}(\overline{P})\right). \tag{7}
$$

After obtaining $\hat{x}_k^s$, the sensor will transmit it as a data packet to the remote estimator. Due to fading and interference, random data drops will occur. As modelled in [6], [8], we assume that the sensor has two transmission power levels: when using a higher energy Δ, the packet will always arrive to the remote estimator; when using a lower energy δ, the successful arrival rate is $\lambda \in (0, 1)$. To simplify the following discussion, we denote the sensor power schedule as:

$$
\theta = \{\gamma_1, \gamma_2, ..., \gamma_k, ...\}, \tag{8}
$$

where $\gamma_k = 1$ or 0 represents that the sensor chooses energy Δ or δ, respectively, at time step k.

B. Remote State Estimation

The transmission of $\hat{x}_k^s$ between the sensor and the remote estimator can be characterized by a binary random process $\{\lambda_k\}, k \in \mathbb{N}$:

$$\lambda_k = \begin{cases} 1, & \text{if } \hat{x}_k^s \text{ arrives at time } k, \\ 0, & \text{otherwise (regarded as dropout).} \end{cases}$$

Denote $\hat{x}_k$ and P_k as the remote estimator's own MMSE state estimate and the corresponding error covariance based on all the sensor data packets received up to time step k. From [20] and [21], the remote state estimate $\hat{x}_k$ obeys the recursion:

$$\hat{x}_k = \begin{cases} \hat{x}_k^s, & \text{if } \lambda_k = 1, \\ A\hat{x}_{k-1}, & \text{if } \lambda_k = 0. \end{cases} \tag{9}$$

The corresponding state estimation error covariance P_k satisfies:

$$P_k = \begin{cases} \overline{P}, & \text{if } \lambda_k = 1, \\ h(P_{k-1}), & \text{if } \lambda_k = 0. \end{cases} \tag{10}$$

Intuitively, higher transmission power leads to better estimation performance. However, in practice, the sensor has a limited energy budget, which motivates us to consider the following optimization problem:

Problem 2.2:

$$\min_{\theta} \quad J(\theta) \triangleq \limsup_{T \to \infty} \frac{1}{T} \sum_{k=1}^{T} \text{Tr}\left(\mathbb{E}[P_k]\right),$$

$$\text{s.t.} \quad \Phi(\theta) \triangleq \limsup_{T \to \infty} \frac{1}{T} \sum_{k=1}^{T} \mathbb{E}\left[\gamma_k \Delta + (1 - \gamma_k)\delta\right] \leqslant \Psi,$$

where Ψ is the average energy constraint for the sensor.

Remark 2.3: We assume that Δ, δ, and Ψ are all positive rational numbers satisfying $\delta < \Psi < \Delta$. $\qquad\square$

III. PRELIMINARIES

In this section, we will revise some preliminary results about the optimal offline schedule and an ACK-based online power schedule when there is no attacker.

A. Optimal Offline Schedule

When the sensor designs its power schedule without utilizing any online information, the optimal solution is provided by the following theorem:

Theorem 3.1 (Optimal Offline Schedule Proposed in [6]): Given the average energy constraint Ψ, suppose that p and q are two co-prime integers satisfying $\frac{p}{q} = \frac{\Psi - \delta}{\Delta - \delta}$. Then the optimal offline power schedule $\theta_{\text{off}}^\star$ to Problem 2.2 over a period q can be constructed in the following form:

$$\underbrace{(1 \underbrace{0 \cdots 0}_{s_0+1 \text{ times}}) \cdots (1 \underbrace{0 \cdots 0}_{s_0+1\text{times}})}_{n \text{ times}} \underbrace{(1 \underbrace{0 \cdots 0}_{s_0 \text{ times}}) \cdots (1 \underbrace{0 \cdots 0}_{s_0\text{times}})}_{m \text{ times}}$$

where 1 and 0 denotes the designed value for γ_k in (8), $m = q - p(s_0 + 1)$, $n = p(s_0 + 2) - q$, and s_0 is the largest integer such that $s_0 \leqslant \frac{q}{p} - 1$. $\qquad\square$

Under the optimal offline schedule $\theta_{\text{off}}^\star$, we have the following closed-form results about the corresponding energy consumption and estimation performance [6].

Proposition 3.2: When $\theta_{\text{off}}^\star$ is used, the average energy cost is given by

$$\Phi(\theta_{\text{off}}^\star) = \frac{(m+n)\Delta + (ms_0 + ns_0 + m)\delta}{ms_0 + ns_0 + 2m + n} = \Psi,$$

and the trace of the expected average state estimation error covariance is given by:

$$J(\theta_{\text{off}}^\star) = \frac{1}{m(s_0 + 2) + n(s_0 + 1)} \cdot$$
$$\text{Tr}\Big\{ m\big[1 + \lambda(s_0 + 1)\big]\overline{P} + n\big[1 + \lambda s_0\big]\overline{P}$$
$$+ m \sum_{i=1}^{s_0+1} \big[1 + \lambda(s_0 + 1 - i)\big](1 - \lambda)^i h^i(\overline{P})$$
$$+ n \sum_{i=1}^{s_0} \big[1 + \lambda(s_0 - i)\big](1 - \lambda)^i h^i(\overline{P})\Big\}.$$

$\qquad\square$

B. Online Power Schedule

The offline power schedules are designed before the system is running without using the realtime measurement or state information. In [9], the author showed that the utilization of the online information can improve the system performance while require less energy consumption. To further improve the estimation performance, an online power schedule based on the ACKs from the remote estimator was proposed in [8] as follows: the remote estimator generates 1-bit ACKs ($= \lambda_k$) to indicate whether the data packet arrives successfully or not and an event-detector at the remote estimator's side collects and stores the ACKs in an L-bit memory. Without loss of generality, assume the sensor uses Δ at the first time step. The memory is set to $11, ..., 11$ initially and the detector randomly chooses to activate z_0-bit memory ($z_0 < L$) with probability μ, or ($z_0 + 1$)-bit memory otherwise. At every time step, the memory shifts all bits one bit to the MSB direction with the existing MSB being deleted and the incoming ACK stored in the LSB. When the memory becomes $00, ..., 00$, the detector sends a flag-ACK to inform the sensor to use high power in the following time step. In the meanwhile, the memory is set to $11, ..., 11$ again (see Fig. 3).

By properly designing the parameter z_0 and μ, the average energy consumption can meet the constraint in Problem 2.2 and the corresponding estimation performance is given by the following theorem:

Theorem 3.3 (Theorem 4.5 in [8]): Under the proposed online power schedule θ_{on}, the trace of the average expected estimation error covariance is given by:

$$J(\theta_{\text{on}}) = \frac{\lambda}{1 - \mu(1 - \lambda)^{z_0+1} - \mu(1 - \lambda)^{z_0+2}} \cdot$$
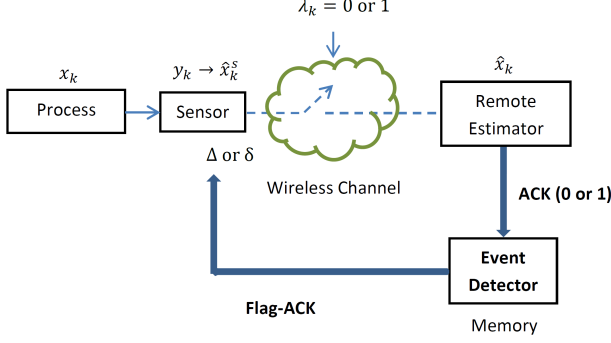$$\text{Tr}\Big[\sum_{i=0}^{z_0} (1 - \lambda)^i h^i(\overline{P}) + \mu(1 - \lambda)^{z_0+1} h^{z_0+1}(\overline{P}) \Big].$$

Fig. 3. System Architecture under Online Sensor Schedule.

□

Compared to the optimal offline schedule, the proposed online schedule θ_{on} has a better estimation performance under the same energy constraint, which is summarized in the following theorem [8]:

Theorem 3.4 (Theorem 5.3 in [8]): Under the same energy constraint as in Problem 2.2, the proposed online schedule θ_{on} has a better estimation performance than the optimal offline schedule $\theta_{\mathrm{off}}^{\star}$ provided in Theorem 3.1, i.e.,

$$J(\theta_{\mathrm{on}}) < J(\theta_{\mathrm{off}}^{\star}).$$

IV. FAKE-ACKNOWLEDGEMENT ATTACK AGAINST REMOTE ESTIMATION

As stated before, the ACK-based online power schedule can improve the estimation performance significantly compared to the offline schedule. However, the simple structure of the 1-bit flag-ACK packet makes it a more reachable (and likely) alternative for the adversary, under both integrity attacks and DoS attacks. In this section, we propose a possible attack pattern for the attacker and investigate the corresponding effect on the estimation performance.

A. Proposed Fake-ACK Attack Pattern

Based on the communication protocol used by the event-detector, the attacker may adopt different types of attacks: when the flag-ACK is sent at every time step with value 1 or 0 (Type A), the attacker modifies the bit contained in the packet to launch the attack, i.e., the integrity attack; when the flag-ACK is sent only when the event happens (Type B), the attacker can simply adopt DoS attack to prevent the transmission of the packet. No matter what types of the communication protocols and attacks are used, the consequent results are the same: the time steps which would use energy Δ now use δ instead under the attack. Therefore, without loss of generality, we will assume that the event-detector adopts protocol Type B and the attacker launches DoS attack in the following discussion (the analysis of the other case is almost the same).

Assume that the attacker also has an energy constraint and cannot launch attack at every time step. Otherwise, it is straightforward to see that the attacker will attack all the flag-ACKs with value 1 to prevent the transmission. Let the proportion of the flag-ACK packets that can be prevented by the attacker among all the flag-ACK packets be constrained to be $\beta \in (0,1)$ and $t, r (t > r)$ are two co-prime integers satisfying $\frac{r}{t} = \beta$. In [15], the optimal DoS attack pattern is proved to be launching the attack consecutively so that the effect on the estimation performance is maximized. This motivates us to consider the specific attack pattern of interest described as follows:

1) the attacker follows a periodic pattern;
2) the attacker maintains a counter and launches DoS attacks to prevent the transmission of the first r coming flag-ACKs, and leave the rest $t - r$ coming flag-ACK with value 1 unchanged;
3) after every t coming flag-ACKs, the counter is set to 0 again.

This is summarized in Algorithm 1.

Algorithm 1 Attacking Pattern for The Attacker

1: Process begins;
2: $counter = 0$;
3: **while** 1 **do**
4:     **if** a flag-ACK packet is sent **then**
5:         **if** $counter \leqslant r$ **then**
6:             block the transmission of the flag-ACK packet;
7:         **else**
8:             do not block;
9:         **end if**
10:         $counter = counter + 1$;
11:     **end if**
12:     **if** $counter == t$ **then**
13:         $counter = 0$;
14:     **end if**
15: **end while**

Example 4.1: We use a simple example to illustrate how this attack pattern works. Assume that $z_0 = 2$, $\beta = \frac{2}{3}$ (thus $r = 2$ and $t = 3$), one possible realization and comparison between the online schedule θ_{on} and the one under attack $\tilde{\theta}_{\mathrm{on}}$ are shown in Fig. 4 (the long arrows represent the arrival packets while the short one is for the dropped packets; the number between arrows is the value of the counter). In the realization of θ_{on} without attack, the second and the third flag-ACK are sent due to two ($z_0 = 2$) consecutive packet losses. When there is an attacker following the pattern in Algorithm 1, it will attack the first two ($r = 2$) flag-ACKs, let the third one transmitted, and reset the counter for a new period.

B. Performance Analysis

Denote the estimation performance of θ_{on} under the proposed fake-ACK attack as $J(\tilde{\theta}_{\mathrm{on}})$. We will investigate the analytical form of $J(\tilde{\theta}_{\mathrm{on}})$ in the following part.

Note that due to the recursion of the dynamics in (10), the covariance P_k can only take value in the infinitely countable set $\{\overline{P}, h(\overline{P}), h^2(\overline{P}), ...\}$. Denote $\tau_k \in \mathbb{Z}$ as the holding
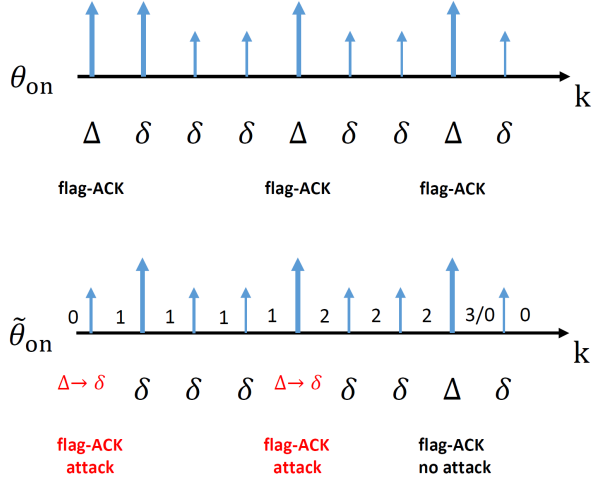
Fig. 4. Comparison between θ_{on} and $\tilde{\theta}_{\text{on}}$

time since the most recent time when the remote estimator successfully received the data from sensor:

$$\tau_k \triangleq k - \max_{1 \leqslant t \leqslant k} \{t : \lambda_t = 1\}. \tag{11}$$

Then we have

$$P_k = \begin{cases} \overline{P}, & \text{if } \lambda_k = 1, \\ h^{\tau_k}(\overline{P}), & \text{if } \lambda_k = 0. \end{cases}$$

Define the value of the attacker's counter at time step k as $\sigma_k \in \{0, 1, 2, ..., t-1\}$ and the state of the process at time step k as:

$$S_k = (\tau_k, \sigma_k).$$

As the strategy of the attacker guarantees that the flag-ACK will be sent to the sensor when the value of the counter is larger than r, the covariance P_k will be bounded and τ_k only takes value in a finite set. Therefore, based on the recursion in (10), it is easy to verify that the process $\{S_k\}$ constitutes a finite state stationary Markov chain.

Remark 4.2: Note that the design of the parameter μ in the online sensor schedule θ_{on} is to tune the activated memory length between z_0 and $z_0 + 1$ in the event-detector to satisfy the energy constraint. When the energy constraint is in some simple form, e.g., $\frac{1}{2}$ or $\frac{1}{3}$, a fixed length activated memory with z_0 is sufficient. Without loss of generality, we assume that the event-detector adopts a fixed activated memory with length z_0 to facilitate the discussion and simplify the notation below. We will later show that our results also apply to the general case with variant length. □

According to the mechanism of the online sensor schedule θ_{on} and the attack strategy, τ_k only takes values in the set $\{0, 1, 2, ..., z_0(\sigma_k + 1)\}$ when $\sigma_k \leqslant r$ and in the set $\{0, 1, 2, ..., z_0\}$ when $r < \sigma_k < t$. Then the state set can be

constructed as:

$$\begin{aligned} \mathcal{S} \triangleq \Big\{ &(0,0), (1,0), .., (z_0-1,0), (z_0,0), \\ &(0,1), (1,1), ..., (2z_0-1,1), (2z_0,1), \\ &... \\ &(0,r), (1,r), ..., (z_0(r+1)-1,r), (z_0(r+1),r), \\ &(0,r+1), (1,r+1), .., (z_0-1,r+1), (z_0,r+1), \\ &(0,r+2), (1,r+2), .., (z_0-1,r+2), (z_0,r+2), \\ &... \\ &(0,t-1), (1,t-1), .., (z_0-1,t-1), (z_0,t-1) \Big\}. \end{aligned}$$

The total number of states can be calculated as:

$$\begin{aligned} |\mathcal{S}| &= \sum_{i=0}^{r} \big[z_0(i+1) + 1 \big] + \big[(t-1) - (r+1) + 1 \big](z_0+1) \\ &= \frac{1}{2} r(r+1) z_0 + t(z_0+1). \end{aligned}$$

It is convenient to label each state ϵ_i in $\mathcal{S}$ in a sequential order from $i = 1$ to $|\mathcal{S}|$. Then we can define the state transition probability matrix as:

$$\mathcal{T}_s = \{T_{ij}\}_{|\mathcal{S}| \times |\mathcal{S}|},$$

where

$$T_{ij} \triangleq \mathbb{P}[S_{k+1} = \epsilon_j | S_k = \epsilon_i].$$

Based on the mechanism of the online sensor schedule θ_{on} and the attack strategy, we can derive the transition probability from $S_{k+1} = (\tau_{k+1}, \sigma_k)$ to $S_k = (\tau_k, \sigma_k)$ as follows:

1) when $\tau_k \mod z_0 \neq 0$ or $\tau_k = 0$, the event detector will not send the flag-ACK (and no attack as a consequence). Thus:

$$\mathbb{P}\big[S_{k+1}|S_k\big] = \begin{cases} \lambda, & \text{if } (\tau_{k+1}, \sigma_{k+1}) = (0, \sigma_k), \\ 1-\lambda, & \text{if } (\tau_{k+1}, \sigma_{k+1}) = (\tau_k+1, \sigma_k), \\ 0, & \text{otherwise;} \end{cases}$$

2) when $\tau_k \mod z_0 = 0$, $\tau_k \neq 0$ and $\sigma_k < r$, the memory satisfies the triggering condition, the flag-ACK will be sent and the attack will be launched with the counter increasing by 1. Thus:

$$\mathbb{P}\big[S_{k+1}|S_k\big] = \begin{cases} \lambda, & \text{if } (\tau_{k+1}, \sigma_{k+1}) = (0, \sigma_k+1), \\ 1-\lambda, & \text{if } (\tau_{k+1}, \sigma_{k+1}) = (\tau_k+1, \sigma_k+1), \\ 0, & \text{otherwise;} \end{cases}$$

3) when $\tau_k \mod z_0 = 0$, $\tau_k \neq 0$ and $r \leqslant \sigma_k < t-1$, the memory satisfies the triggering condition, the flag-ACK will be sent without being attacked and the counter increasing by 1. Thus:

$$\mathbb{P}\big[S_{k+1}|S_k\big] = \begin{cases} 1, & \text{if } (\tau_{k+1}, \sigma_{k+1}) = (0, \sigma_k+1), \\ 0, & \text{otherwise;} \end{cases}$$

4) when $\tau_k \mod z_0 = 0$, $\tau_k \neq 0$ and $\sigma_k = t-1$, the memory satisfies the triggering condition, the flag-ACK will be sent without being attacked and the counter is reset to 0. Thus:

$$\mathbb{P}\big[S_{k+1}|S_k\big] = \begin{cases} 1, & \text{if } (\tau_{k+1}, \sigma_{k+1}) = (0, 0), \\ 0, & \text{otherwise.} \end{cases}$$

Based on the above discussion, we can obtain the expression of the transition matrix $\mathcal{T}_s$. Due to space limitation, we provide a simple example of $\mathcal{T}_s$ when $z_0 = 2$, $r = 1$ and $t = 3$ (therefore $|\mathcal{S}| = 11$) in (12).

Based on the well-established ergodic Markov chain theory [22], $\{S_k\}$ has a stationary probability distribution of states, which is denoted as:

$$\Pi = \left[\mathbb{P}[\epsilon_1], \mathbb{P}[\epsilon_2], ..., \mathbb{P}[\epsilon_{|\mathcal{S}|}]\right]',$$

When $\{S_k\}$ enters the steady state, we have

$$\begin{cases} \mathcal{T}_s \Pi = \Pi, \\ \sum_{i=1}^{|\mathcal{S}|} \Pi(i) = 1, \end{cases} \tag{13}$$

where $\Pi(i)$ is the i-th element of Π.

By solving (13), we can obtain the stationary distribution of state, denoted as $\Pi^\star$. Then we can calculate the estimation performance of θ_{on} under the proposed fake-ACK attack as follows:

$$\begin{aligned} J(\tilde{\theta}_{\mathrm{on}}) &= \limsup_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} \mathrm{Tr}\left(\mathbb{E}[P_k]\right) \\ &= \limsup_{k\to\infty} \mathrm{Tr}\left(\mathbb{E}[P_k]\right) \\ &= \sum_{i=1}^{|\mathcal{S}|} \Pi^\star(i) \mathrm{Tr}\left(\mathbb{E}\left[P_k(\epsilon_i)\right]\right). \end{aligned}$$

C. Discussion

To analyze the effect of the proposed attacking pattern on θ_{on}, we first consider two extreme cases.

When the energy constraint for the attacker is $\beta = 1$, the attacker can block the transmissions of all the flag-ACKs, resulting in the sensor using the low power δ within the entire time-horizon. The corresponding estimation performance can be calculated as:

$$\begin{aligned} J(\tilde{\theta}_{\mathrm{on}})_{\max} &= \limsup_{T\to\infty} \frac{1}{T} \sum_{k=1}^{T} \mathrm{Tr}\left(\mathbb{E}[P_k]\right) \\ &= \limsup_{k\to\infty} \mathrm{Tr}\left(\mathbb{E}[P_k]\right) \\ &= \sum_{i=0}^{+\infty} \lambda(1-\lambda)^i \mathrm{Tr}\left(h^i(\overline{P})\right). \end{aligned}$$

Note that the necessary and sufficient condition for the stability of the above case is simply given by $\rho(A)(1-\lambda) < 1$, where $\rho(A)$ is the maximum eigenvalue of A. Since, as proved in [20] and [6], more energy budget is always beneficial, we have:

$$J(\tilde{\theta}_{\mathrm{on}})_{\max} = J(\theta_{\mathrm{off}}^\star)_{(n=0)} \geqslant J(\theta_{\mathrm{off}}^\star), \tag{14}$$

where n is the number of high energy δ that can be used within each period of $J(\theta_{\mathrm{off}}^\star)$ defined in Theorem 3.1.

One the other hand, when $\beta = 0$, the attacker cannot block any flag-ACK and the online sensor schedule will operate normally. Therefore, we have:

$$J(\tilde{\theta}_{\mathrm{on}})_{\min} = J(\theta_{\mathrm{on}}). \tag{15}$$

Combining (14) and (15), we have:

$$J(\theta_{\mathrm{on}}) = J(\tilde{\theta}_{\mathrm{on}})_{\min} \leqslant J(\theta_{\mathrm{off}}^\star) \leqslant J(\tilde{\theta}_{\mathrm{on}})_{\max}.$$

As a consequence, when the capability of the attacker is limited, keeping the online schedule will still guarantee a better performance than the offline schedule $\theta_{\mathrm{off}}^\star$. Otherwise, when the attacker has sufficient energy budget, the estimation performance under the online sensor schedule θ_{on}, $J(\tilde{\theta}_{\mathrm{on}})$, will be even worse than the offline schedule $\theta_{\mathrm{off}}^\star$. In such case, not using ACK is preferable to using fake ACK and the reasonable choice for the sensor is to adopt the offline schedule rather than keeping the online schedule. Furthermore, as the performance metric $J(\tilde{\theta}_{\mathrm{on}})$ is growing with the energy budget β, there exists a threshold value $\overline{\beta}$ such that (as later shown in Fig. 6):

$$J(\tilde{\theta}_{\mathrm{on}})_{\beta=\overline{\beta}} = J(\theta_{\mathrm{off}}^\star).$$

Hence, in practice, based on the information about the attacker's capability, the sensor can choose different types of schedules to obtain a better performance, i.e.,

$$\tilde{\theta}_{\mathrm{on}} = \begin{cases} \theta_{\mathrm{on}}, & \text{when } \beta < \overline{\beta}, \\ \theta_{\mathrm{off}}^\star, & \text{when } \beta \geqslant \overline{\beta}, \end{cases}$$

where $\overline{\beta}$ can be calculated numerically. How to obtain the value of $\overline{\beta}$ analytically is an interesting problem which will be considered in our future work.

Remark 4.3: Note that the sensor can detect the existence of the attacker by checking the arrival rate of flag-ACKs based on the theoretical arrival rate provided in [8]. The observation will enable the sensor to estimate the capability of the attacker. On the other hand, when the sensor is aware of the existence of the attacker, the attacker will also need to re-design his strategy to avoid being detected, which will result in a dynamic decision-making process between both sides. We will investigate this problem under a game-theoretic framework in the future. $\square$

V. SIMULATION

In this section, we provide numerical examples to illustrate our results in different situations.

Define

$$J_k(\theta) = \frac{1}{k} \sum_{i=1}^{k} \mathrm{Tr}\left(\mathbb{E}[P_i]\right),$$

as the empirical approximation (via 100000 Monte Carlo simulations) of $J(\theta)$ at every time instant k.

Consider a scalar system with parameters $A = 1.2$, $C = 0.7$, $R = Q = 0.8$, $\lambda = 0.5$. Suppose that the energy constraint for the sensor is given by $\Psi = \frac{1}{7}\Delta + \frac{6}{7}\delta$. It is easy to verify that the optimal offline schedule is given in a periodic form of $\{1000000, 1000000, ...\}$ with performance $J(\theta_{\mathrm{off}}^\star) = 2.0953$. The parameter for the online schedule is $z_0 = 2$ with performance $J(\theta_{\mathrm{on}}) = 1.6399$. As shown in Fig. 5, when the energy constraint for the attacker is $\beta = \frac{1}{5}$, the estimation performance $J(\tilde{\theta}_{\mathrm{on}})$ is better than the performance using the offline schedule $\theta_{\mathrm{off}}^\star$ (thus the sensor may still choose θ_{on}). However, when the energy budget for the attacker is further increased, e.g., $\beta = \frac{2}{3}$, $J(\tilde{\theta}_{\mathrm{on}})$ is worse even than the offline $\theta_{\mathrm{off}}^\star$ (thus the sensor may switch from the online schedule to the

$$\mathcal{T}_s = \begin{bmatrix} \lambda & \lambda & \lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1-\lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1-\lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \lambda & \lambda & 0 & \lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1-\lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1-\lambda & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1-\lambda & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1-\lambda & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & \lambda & \lambda & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\lambda & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\lambda & 0 \end{bmatrix} \tag{12}$$

offline one to obtain better estimation performance). In Fig. 6, the comparison of $J(\tilde{\theta}_{\text{on}})$ as a function of β is provided. As we can see, the approximate value of $\overline{\beta}$ is about 0.28.
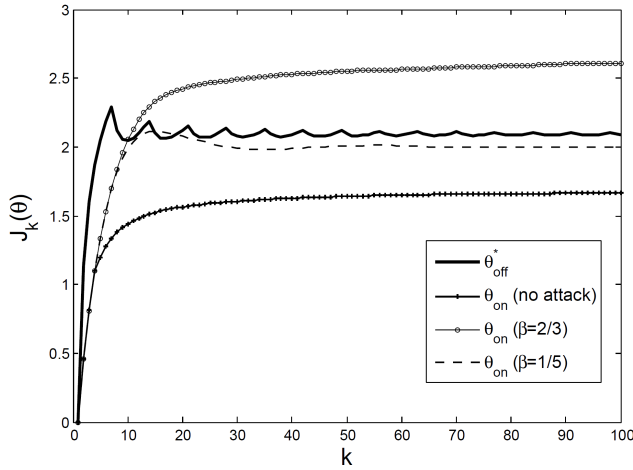

Fig. 5. Comparison between $J(\theta_{\text{off}}^\star)$, $J(\theta_{\text{on}})$ and $J(\tilde{\theta}_{\text{on}})$.

Fig. 6. Comparison of $J(\tilde{\theta}_{\text{on}})$ under different β.

VI. Conclusion

In this work, a potential class of malicious attacks against remote state estimation was studied. We proposed a strategy for the attacker which can modify the flag-ACKs from the remote estimator and convey fake information to the sensor. The corresponding effect on the estimation performance is analyzed based on well-established Markov chain theory. The condition for the sensor to use an online schedule instead of an offline schedule is provided. Simulations were provided to illustrate our results. Future works include obtaining the threshold value of $\overline{\beta}$ analytically, considering other types of fake-ACK attacks and extending the problem into a game-theoretic framework where the attacker need to design their pattern without being detected.

References

[1] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

[2] V. C. Gungor and G. P. Hancke, "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 10, pp. 4258–4265, 2009.

[3] D. E. Quevedo, A. Ahlén, A. S. Leong, and S. Dey, "On Kalman filtering over fading wireless channels with controlled transmission powers," *Automatica*, vol. 48, no. 7, pp. 1306–1316, 2012.

[4] O. C. Imer and T. Başar, "Optimal estimation with limited measurements," in *Proceedings of the IEEE Conference on Decision and Control and the European Control Conference*, 2005, pp. 1029–1034.

[5] A. Leong and S. Dey, "Power allocation for error covariance minimization in Kalman filtering over packet dropping links," in *IEEE 51st Annual Conference on Decision and Control (CDC)*, Dec 2012, pp. 3335–3340.

[6] L. Shi, P. Cheng, and J. Chen, "Sensor data scheduling for optimal state estimation with communication energy constraint," *Automatica*, vol. 47, no. 8, pp. 1693–1698, 2011.

[7] Y. Li, D. E. Quevedo, V. Lau, and L. Shi, "Online sensor transmission power schedule for remote state estimation," in *IEEE 52nd Aunnal Conference on Decision and Control (CDC), Florence, Italy*, 2013.

[8] D. Han, P. Cheng, J. Chen, and L. Shi, "An online sensor power schedule for remote state estimation with communication energy constraint," *IEEE Transactions on Automatic Control*, vol. 59, no. 7, pp. 1942–1947, 2014.

[9] J. Wu, K. Johansson, and L. Shi, "An improved hybrid sensor schedule for remote state estimation under limited communication resources," in *Proceedings of the 51st IEEE Conference on Decision and Control*, 2012, pp. 3305–3310.

[10] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[11] A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *28th International Conference on Distributed Computing Systems Workshops*, 2008, pp. 495–500.

[12] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[13] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in *Proceedings of the 1st international conference on High Confidence Networked Systems*. ACM, 2012, pp. 47–54.

[14] Y. Li, L. Shi, P. Cheng, J. Chen, and D. E. Quevedo, "Jamming attack on cyber-physical systems: A game-theoretic approach," in *IEEE International Conference on CYBER Technology in Automatation, Control, and Intelligent Systems, Nanjing, China*, 2013.

[15] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack policy against remote state estimation," in *IEEE 52nd Annual Conference on Decision and Control (CDC)*. IEEE, 2013, pp. 5444–5449.

[16] C.-Z. Bai and V. Gupta, "On Kalman filtering in the presence of a compromised sensor: Fundamental performance bounds," in *American Control Conference*. IEEE, 2014, pp. 3029–3034.

[17] P. Hovareshti, V. Gupta, and J. S. Baras, "Sensor scheduling using smart sensors," in *Proceedings of the 46th IEEE Conference on Decision and Control*, 2007, pp. 494–499.

[18] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, 2004.

[19] L. Shi, K. H. Johansson, and L. Qiu, "Time and event-based sensor scheduling for networks with limited communication resources," in *World Congress of the International Federation of Automatic Control (IFAC)*, vol. 18, no. 1, 2011, pp. 13 263–13 268.

[20] Y. Li, D. E. Quevedo, V. Lau, and L. Shi, "Optimal periodic transmission power schedules for remote estimation of ARMA processes," *IEEE Transactions on Signal Processing*, vol. 61, no. 24, pp. 6164–6174, 2013.

[21] L. Shi, M. Epstein, and R. M. Murray, "Kalman filtering over a packet-dropping network: A probabilistic perspective," *IEEE Transactions on Automatic Control*, vol. 55, no. 3, pp. 594–604, 2010.

[22] J. R. Norris, *Markov chains*. Cambridge University Press, 1998, no. 2.